

#2

11017 U.S. PTO
10/024075
12/17/01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of : **Hideaki NEGAWA**
Filed: : **Concurrently herewith**
For: : **MULTICAST COMMUNICATION SYSTEM**
Serial No. : **Concurrently herewith**

Assistant Commissioner for Patents
Washington, D.C. 20231

December 17, 2001

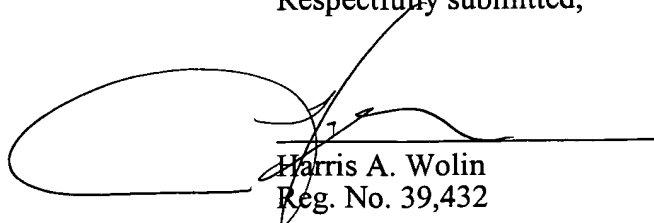
PRIORITY CLAIM AND
SUBMISSION OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **JAPANESE** patent application no. **2001-258890** filed **August 29, 2001**, a certified copy of which is enclosed.

Any fee, due as a result of this paper, not covered by an enclosed check, may be charged to Deposit Acct. No. 50-1290.

Respectfully submitted,



Harris A. Wolin
Reg. No. 39,432

ROSENMAN & COLIN, LLP
575 MADISON AVENUE
IP Department
NEW YORK, NEW YORK 10022-2584
DOCKET NO.: FUJH 19.264
TELEPHONE: (212) 940-8800

日本国特許庁
JAPAN PATENT OFFICE

#2
J1017 U.S. PRO
10/024075
12/17/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:

2001年 8月29日

出願番号
Application Number:

特願2001-258890

出願人
Applicant(s):

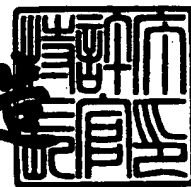
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年10月19日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3091480

【書類名】 特許願

【整理番号】 0151296

【提出日】 平成13年 8月29日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/00
H04H 1/00
H04L 12/14

【発明の名称】 マルチキャスト通信システム

【請求項の数】 5

【発明者】
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 子川 英昭

【特許出願人】
【識別番号】 000005223
【氏名又は名称】 富士通株式会社

【代理人】
【識別番号】 100094514
【弁理士】
【氏名又は名称】 林 恒▲徳▼

【代理人】
【識別番号】 100094525
【弁理士】
【氏名又は名称】 土井 健二

【手数料の表示】
【予納台帳番号】 030708
【納付金額】 21,000円

【提出物件の目録】
【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704944

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 マルチキャスト通信システム

【特許請求の範囲】

【請求項 1】 所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと、マルチキャストグループに属し、前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって、

前記マルチキャストサーバは、

前記データを第 1 の暗号化鍵により暗号化するデータ暗号部と、

前記データ暗号部により暗号化されたデータを、前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と、

前記第 1 の暗号化鍵を第 2 の暗号化鍵により暗号化する鍵暗号部と、

前記鍵暗号部により暗号化された第 1 の暗号化鍵を、前記マルチキャストグループに属するクライアントのうち、前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と、

を備え、

前記複数のクライアントのうち、前記データ配信サービスに加入したクライアントは、

前記鍵送信部により送信される、暗号化された第 1 の暗号化鍵を受信する鍵受信部と、

前記鍵受信部により受信された、暗号化された第 1 の暗号化鍵を復号化鍵により復号化する鍵復号部と、

前記データ送信部により送信される、暗号化されたデータを、前記鍵復号部により得られた第 1 の暗号化鍵により復号するデータ復号部と、

を備えているマルチキャスト通信システム。

【請求項 2】 所定のデータ配信サービスに関するデータを第 1 の暗号化鍵により暗号化するデータ暗号部と、

前記データ暗号部により暗号化されたデータをマルチキャストにより、所定のマルチキャストグループに属するクライアントにマルチキャストにより送信する

データ送信部と、

前記第1の暗号化鍵を第2の暗号化鍵により暗号化する鍵暗号部と、

前記鍵暗号部により暗号化された第1の暗号化鍵を、前記マルチキャストに属するクライアントのうち、前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と、

を備えているマルチキャストデータ送信装置。

【請求項3】 マルチキャストにより送信される、所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信装置であって、

前記データ配信サービスに加入することにより得られる暗号化された第1の暗号化鍵を復号化する鍵復号部と、

前記データ配信サービスに関するデータが前記第1の暗号化鍵により暗号化されたものを受信するデータ受信部と、

前記データ受信部により受信された、暗号化されたデータを、前記鍵復号部の復号化により得られた第1の暗号化鍵により復号化するデータ復号部と、

を備えているマルチキャストデータ受信装置。

【請求項4】 所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと、マルチキャストグループに属し、前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって、

前記マルチキャストサーバは、

前記データを暗号化するためのデータ暗号化鍵を、所定の更新タイミングごとに、該更新タイミング前に有効なデータ暗号化鍵に、該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある、更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と、

前記更新鍵を生成し、または、あらかじめ保持する更新鍵保持部と、

前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と、

前記データ暗号部により暗号化されたデータを、前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と、

前記更新タイミングごとに、更新タイミング後に有効なデータ暗号化鍵に対応

する更新鍵を、該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と、

前記更新タイミングごとに、前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と

を備え、

前記複数のクライアントのうち、前記データ配信サービスに加入したクライアントは、

前記データ送信部により送信される、暗号化されたデータを受信するデータ受信部と、

前記データ受信部により受信される、前記暗号化されたデータを、前記現在有効なデータ暗号化鍵と同一の現在有効なデータ復号化鍵により復号化するデータ復号部と、

前記更新鍵送信部により送信される、暗号化された更新鍵を受信する更新鍵受信部と、

前記更新鍵受信部により受信される、暗号化された更新鍵を、前記現在有効なデータ復号化鍵により復号化する更新鍵復号部と、

前記データ配信サービスへの加入時には、外部から与えられ、その後は、前記更新タイミングごとに、該更新タイミング前に有効なデータ復号化鍵に、該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより、更新タイミング後に有効なデータ復号化鍵を生成し、前記更新タイミングごとに、前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新するデータ復号化鍵更新部と、

を備えているマルチキャスト通信システム。

【請求項 5】 所定のデータ配信サービスに関するデータを暗号化するためのデータ暗号化鍵を、所定の更新タイミングごとに、該更新タイミング前に有効なデータ暗号化鍵に、該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある、更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と、

前記更新鍵を生成し、または、あらかじめ保持する更新鍵保持部と、

前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と、

前記データ暗号部により暗号化されたデータを、所定のマルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と、

前記更新タイミングごとに、更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を、該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と、

前記更新タイミングごとに、前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と

を備えているマルチキャストデータ送信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、マルチキャスト通信システムに関し、具体的には、所定のデータ配信サービスに関するデータをマルチキャストにより通信するマルチキャスト通信システムに関する。また、本発明は、マルチキャストデータ送信装置およびマルチキャストデータ受信装置に関する。

【0002】

【従来の技術】

インターネットまたはイントラネットにおいて、多数のクライアント（マルチキャストグループに属するクライアント）に同じデータを配信する周知の技術として、IPマルチキャスト（IP Multicast）がある。このIPマルチキャストは、インターネットまたはイントラネット上で音楽、映像等のデータ（コンテンツ）を配信するのに適している。今後、コンテンツの配信にIPマルチキャストの利用が盛んになれば、クライアントに対して課金を行い、データ配信サービス料（受信料）を徴収したいという要望が生まれることが予測される。

【0003】

その際に、課金を適切に行うために、IPマルチキャストグループに属するク

ライアントのうち、データ配信サービスに加入したクライアントは配信データを視聴または聴視できる一方、データ配信サービスに加入していないクライアントは配信データを受信するものの、視聴および聴視できないようにする必要がある。

【 0 0 0 4 】

このためには、データの配信元が、クライアントのデータ配信サービスへの加入／非加入を正確に把握することが重要となり、また、加入したクライアントのみが配信データを視聴または聴視できるための暗号化技術が重要となる。

【 0 0 0 5 】

さらに、課金の方法としては、受信者が多数であることから、受信したデータ量に応じて課金を行える従量制課金が望ましいと考えられる。

【 0 0 0 6 】

【発明が解決しようとする課題】

しかし、現在インターネット上で実現されている暗号化技術は、データの送信者と受信者とが1対1（ユニキャスト）であることを前提としている。このため、多数の受信者を対象とするIPマルチキャストに関しては考慮がなされておらず、IPマルチキャストでは、暗号化されていないデータが配信されてしまうのが現状である。

【 0 0 0 7 】

また、従来の従量制課金方式としては、CS放送等で採用されているペーパービュー（Pay per View）方式があるが、この方式は番組プログラム単位で課金を行うものである。したがって、番組プログラムの途中で視聴を中止したとしても番組全体を視聴した料金が課金される。このため、厳密には受信したデータ量で課金を行っているとは言えない。

【 0 0 0 8 】

インターネット上で画像や音楽を配信する場合には、プログラム単位よりも短い単位で受信者が加入／脱退することが考えられ、課金方式としても現状のペーパービュー方式よりもきめの細かい方式が要求される。

【 0 0 0 9 】

本発明は、このような背景に鑑みなされたものであり、その目的は、マルチキャスト通信において暗号化および復号化を適切に行えるようにすることにある。

【 0 0 1 0 】

また、本発明の目的は、マルチキャストグループに属するクライアントのうち、データ配信サービスに加入しているクライアントを把握可能とすることにある。

【 0 0 1 1 】

さらに、本発明の目的は、従量制課金を適切に行うことにある。

【 0 0 1 2 】

【課題を解決するための手段】

前記目的を達成するために、本発明の第1の側面によるマルチキャスト通信システムは、所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと、マルチキャストグループに属し、前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって、前記マルチキャストサーバは、前記データを第1の暗号化鍵により暗号化するデータ暗号部と、前記データ暗号部により暗号化されたデータを、前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と、前記第1の暗号化鍵を第2の暗号化鍵により暗号化する鍵暗号部と、前記鍵暗号部により暗号化された第1の暗号化鍵を、前記マルチキャストグループに属するクライアントのうち、前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と、を備え、前記複数のクライアントうち、前記データ配信サービスに加入したクライアントは、前記鍵送信部により送信される、暗号化された第1の暗号化鍵を受信する鍵受信部と、前記鍵受信部により受信された、暗号化された第1の暗号化鍵を復号化鍵により復号化する鍵復号部と、前記データ送信部により送信される、暗号化されたデータを、前記鍵復号部により得られた第1の暗号化鍵により復号するデータ復号部と、を備えている。

【 0 0 1 3 】

本発明の第1の側面によるマルチキャストデータ送信装置は、所定のデータ配

信サービスに関するデータを第 1 の暗号化鍵により暗号化するデータ暗号部と、前記データ暗号部により暗号化されたデータをマルチキャストにより、所定のマルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と、前記第 1 の暗号化鍵を第 2 の暗号化鍵により暗号化する鍵暗号部と、前記鍵暗号部により暗号化された第 1 の暗号化鍵を、前記マルチキャストに属するクライアントのうち、前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と、を備えている。

【 0 0 1 4 】

本発明の第 1 の側面によるマルチキャストデータ受信装置は、マルチキャストにより送信される、所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信装置であって、前記データ配信サービスに加入することにより得られる暗号化された第 1 の暗号化鍵を復号化する鍵復号部と、前記データ配信サービスに関するデータが前記第 1 の暗号化鍵により暗号化されたものを受信するデータ受信部と、前記データ受信部により受信された、暗号化されたデータを、前記鍵復号部の復号化により得られた第 1 の暗号化鍵により復号化するデータ復号部と、を備えている。

【 0 0 1 5 】

本発明の第 1 の側面によると、前記マルチキャストサーバ（またはマルチキャストデータ送信装置）は、前記データの暗号化に用いられる第 1 の暗号化鍵を第 2 の暗号化鍵により暗号化して、前記マルチキャストグループに属するクライアントのうち、前記データ配信サービスに加入したクライアント（またはマルチキャストデータ受信装置）にユニキャストにより送信する。前記データ配信サービスに加入したクライアントは、前記ユニキャストにより送信される、暗号化された第 1 の暗号化鍵を受信すると、これを復号化鍵により復号化する。続いて、前記マルチキャストサーバは、前記データを前記第 1 の暗号化鍵により暗号化して、前記マルチキャストグループに属するクライアントにマルチキャストにより送信する。前記クライアントは、前記暗号化されたデータを受信すると、これを前記復号化鍵の復号化により得られた前記第 1 の暗号化鍵により復号化する。

【 0 0 1 6 】

本発明の第1の側面によると、所定のデータ配信サービスに関するデータが暗号化される。また、該サービスに加入したクライアントのみが、暗号化されたデータを復号化できる一方、該サービスに加入していないクライアントに対してはデータの機密性が確保される。したがって、マルチキャスト通信において、データの暗号化を適切に行うことができる。

【 0 0 1 7 】

本発明の第2の側面によるマルチキャスト通信システムは、所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと、マルチキャストグループに属し、前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって、前記マルチキャストサーバは、前記データを暗号化するためのデータ暗号化鍵を、所定の更新タイミングごとに、該更新タイミング前に有効なデータ暗号化鍵に、該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある、更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と、前記更新鍵を生成し、または、あらかじめ保持する更新鍵保持部と、前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と、前記データ暗号部により暗号化されたデータを、前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と、前記更新タイミングごとに、更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を、該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と、前記更新タイミングごとに、前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と、を備え、前記複数のクライアントのうち、前記データ配信サービスに加入したクライアントは、前記データ送信部により送信される、暗号化されたデータを受信するデータ受信部と、前記データ受信部により受信される、前記暗号化されたデータを、前記現在有効なデータ暗号化鍵と同一の現在有効なデータ復号化鍵により復号化するデータ復号部と、前記更新鍵送信部により送信される、暗号化された更新鍵を受信する更新鍵受信部と、前記更新鍵受信部により受信される、暗号化された更新鍵を、前記現在有効なデータ復号化鍵により復号化する更新鍵復号部と、前記データ配信

サービスへの加入時には、外部から与えられ、その後は、前記更新タイミングごとに、該更新タイミング前に有効なデータ復号化鍵に、該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより、更新タイミング後に有効なデータ復号化鍵を生成し、前記更新タイミングごとに、前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新するデータ復号化鍵更新部と、を備えている。

【 0 0 1 8 】

本発明の第2の側面によるマルチキャストデータ送信装置は、所定のデータ配信サービスに関するデータを暗号化するためのデータ暗号化鍵を、所定の更新タイミングごとに、該更新タイミング前に有効なデータ暗号化鍵に、該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある、更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と、前記更新鍵を生成し、または、あらかじめ保持する更新鍵保持部と、前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と、前記データ暗号部により暗号化されたデータを、所定のマルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と、前記更新タイミングごとに、更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を、該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と、前記更新タイミングごとに、前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と、を備えている。

【 0 0 1 9 】

本発明の第2の側面によると、前記マルチキャストサーバ（またはマルチキャストデータ送信装置）は、前記データを現在有効なデータ暗号化鍵により暗号化して、前記マルチキャストグループに属するクライアントにマルチキャストにより送信する。前記クライアントは、前記マルチキャストサーバから送信される、暗号化されたデータを受信して、前記暗号化されたデータを前記現在有効なデータ暗号化鍵と同一の現在有効な復号化鍵により復号化する。前記マルチキャストサーバは、前記データ暗号化鍵を、所定の更新タイミングごとに、該更新タイミ

ング前に有効なデータ暗号化鍵に、該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある、更新タイミング後に有効となるデータ暗号化鍵に更新する。前記マルチキャストサーバは、前記更新タイミングごとに、更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を、該更新タイミング後に有効なデータ暗号化鍵により暗号化して、前記クライアントにユニキャストまたはマルチキャストにより送信する。前記クライアントは、前記マルチキャストサーバから送信される、暗号化された更新鍵を受信して、該暗号化された更新鍵を、前記現在有効なデータ復号化鍵により復号化する。前記クライアントは、前記データ配信サービスへの加入時には、外部から与えられ、その後は、前記更新タイミングごとに、該更新タイミング前に有効なデータ復号化鍵に、該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより、更新タイミング後に有効なデータ復号化鍵を生成し、前記更新タイミングごとに、前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新する。

【 0 0 2 0 】

本発明の第2の側面によっても、前述した第1の側面と同様の作用効果を得ることができる。

【 0 0 2 1 】

【発明の実施の形態】

以下に、本発明の実施の形態について図面を参照しながら説明するが、これらは例であって、本発明の技術的範囲を限定するものではない。

【 0 0 2 2 】

1. 第1の実施の形態

図1は、本発明の第1の実施の形態によるマルチキャスト通信システムの全体構成を示すブロック図である。このマルチキャスト通信システムは、インターネット1に接続されたマルチキャストサーバ2と、複数のクライアント3a～3dを有するマルチキャストグループ3とを備えている。

【 0 0 2 3 】

マルチキャストサーバ（以下、単に「サーバ」という。）2は、データ配信サ

ービスを行うサーバであり、音楽、映像、テキスト等の配信データ（コンテンツ）を保持し、このコンテンツをインターネット1を介してIPマルチキャストによりマルチキャストグループ3に属するクライアント3a～3dに配信する。

【0024】

クライアント3a～3dは、マルチキャストグループ3に属し、サーバ2からIPマルチキャストにより送信された配信データを受信する。図1では、クライアントの個数を、一例として4つにしているが、4つ以外の個数であってもよい。

【0025】

このマルチキャスト通信システムでは、マルチキャストグループ3に属するクライアント3a～3dのうち、所定の加入手続（後述）を経てサーバ2のデータ配信サービスに加入したもの（加入者）だけが、このデータ配信サービスを受けることができるようになっている。これは、サーバ2が配信データを暗号化して送信するとともに、マルチキャストグループ3に属するクライアントが所定の加入手続を経てデータ配信サービスの加入者となり、暗号化された配信データを復号化するための復号鍵（共通鍵であり、以下「グループセッション鍵Kgr」という。）を入手することにより実現される。

【0026】

すなわち、クライアント3a～3dは、マルチキャストグループ3に属するので、いずれのクライアントもサーバ2からのデータ配信サービスに関する配信データを受信するが、所定の加入手続を経て加入者とならなければ、受信した配信データを復号化して、その配信データを視聴、聴視等することができないようになっている。

【0027】

また、このマルチキャスト通信システムでは、データ配信サービスの加入者に対して、従量制による課金が行なわれる。この従量制による課金は、本実施の形態では、データ配信サービスに加入してからの時間によってなされる。

【0028】

以下、サーバ2、クライアント3a～3d、およびこれらが行う処理の詳細に

ついて説明する。

【 0 0 2 9 】

図 2 は、サーバ 2 の構成を示すブロック図である。サーバ 2 は、制御部 2 0、データ暗号部 2 1、鍵暗号部 2 2、送受信部 2 3、コンテンツデータベース 2 4、および加入者リストデータベース 2 5 を備えている。

【 0 0 3 0 】

制御部 2 0 は、データ暗号部 2 1、鍵暗号部 2 2、送受信部 2 3、コンテンツデータベース 2 4、および加入者リストデータベース 2 5 を制御するとともに、後に詳述する加入者の加入および脱退の処理、加入に伴うグループセッション鍵 Kgr の配布、従量制による課金等の処理を行う。また、制御部 2 0 は、グループセッション鍵 Kgr を保持し、データ暗号部 2 1 および鍵暗号部 2 2 に暗号化処理を実行させる際に、これらデータ暗号部 2 1 および鍵暗号部 2 2 にグループセッション鍵 Kgr を与える。

【 0 0 3 1 】

コンテンツデータベース 2 4 は、ハードディスク、半導体メモリ等の記憶装置、または、DVD、CD 等の記録媒体およびその読み取り装置により構成され、マルチキャストグループ 3 に送信される配信データ（コンテンツ）を記憶する。このコンテンツデータベース 2 4 は、制御部 2 0 の制御の下、配信データをデータ暗号部 2 1 に与える。

【 0 0 3 2 】

データ暗号部 2 1 は、グループセッション鍵（共通鍵）Kgr を制御部 2 0 から受け取り、制御部 2 0 の制御の下、コンテンツデータベース 2 4 からの配信データをグループセッション鍵 Kgr により暗号化して送受信部 2 3 に与える。暗号化の方法としては、DES（Data Encryption Standard）等が用いられる。なお、グループセッション鍵 Kgr は、データ暗号部 2 1 が保持していてもよい。

【 0 0 3 3 】

加入者リストデータベース 2 5 は、ハードディスク、半導体メモリ等の記憶装置、または、DVD、CD 等の記録媒体およびその読み取り／書き込み装置により構成され、図 3 に示す加入者リストを記憶する。加入者リストは、マルチキャ

ストグループ3に属するクライアント3a～3dのうち、所定の加入手続を経て、サーバ2のデータ配信サービスに加入したクライアントのリストである。この加入者リストに登録された加入者は、グループセッション鍵K_{gr}をサーバ2から提供され、これにより、サーバ2からの暗号化された配信データを復号化することができる。

【0034】

図3に示すように、加入者リストを構成する各リストセルは、加入者名、鍵復号鍵K_m、および加入日時を有する。

【0035】

「加入者名」は、あるクライアントを他のクライアントからユニークに識別するための名称、識別子等であり、この加入者名としては、たとえば、データ配信サービスの提供者が加入者に与えるユニークなユーザID、そのクライアントのIPアドレス等が使用される。

【0036】

「鍵復号鍵」は、グループセッション鍵K_{gr}を暗号化し、かつ、暗号化されたグループセッション鍵K_{gr}（以下「暗号化グループセッション鍵K_{gr}x」という。）を復号化するための共通鍵である。この鍵復号鍵は、加入者も所有する。各加入者に対してそれぞれ個別の鍵復号鍵K_m(A)、K_m(B)等が設けられることが好ましい。

【0037】

「加入日時」は、加入者がデータ配信サービスに加入した日時である。本実施の形態では、この加入日時から脱退日時までの時間に基づいて、各加入者から徴収する料金（データ配信サービス料）が計算される。

【0038】

マルチキャストグループ3に属するクライアントがデータ配信サービスに新たに加入すると、制御部20は、新たなリストセルを生成し、生成したリストセルを加入者リストに追加する。一方、既に加入者となっているクライアントがデータ配信サービスから脱退すると、制御部20は、脱退した加入者のリストセルを加入者リストから消去（削除）する。

【 0 0 3 9 】

鍵暗号部 2 2 は、制御部 2 0 からグループセッション鍵 K_{gr} を受け取り、制御部 2 0 の制御の下、送信先のクライアントの鍵復号鍵 K_m を加入者リストから読み出し、読み出した鍵復号鍵 K_m によりグループセッション鍵 K_{gr} を暗号化する。暗号化の方法としては、DES (Data Encryption Standard) 等が用いられる。そして、鍵暗号部 2 2 は、暗号化により得られた暗号化グループセッション鍵 K_{grx} を送受信部 2 3 に与える。たとえば、クライアント 3 a にグループセッション鍵 K_{gr} を送信する場合に、鍵暗号部 2 2 は、グループセッション鍵 K_{gr} をクライアント 3 a の鍵復号鍵 $K_m(A)$ を用いて暗号化する。

【 0 0 4 0 】

送受信部 2 3 は、インターネット 1 とのインタフェース装置である。この送受信部 2 3 は、制御部 2 0 の制御の下、データ暗号部 2 1 からのデータをマルチキャストグループ 3 に属するクライアントにインターネット 1 を介して IP マルチキャストにより送信するとともに、鍵暗号部 2 2 からの暗号化グループセッション鍵 K_{grx} をインターネット 1 を介してユニキャストによりクライアントに送信する。また、送受信部 2 3 は、マルチキャストグループ 3 に属するクライアントからインターネット 1 を介して送信されてきたデータを受信し、制御部 2 0 に与える。

【 0 0 4 1 】

クライアント 3 a ~ 3 d には、サーバ 2 からの配信データを受信するためのハードウェア装置として、配信データ受信装置（またはアダプタ）が取り付けられる。この配信データ受信装置は、たとえば市販されることにより、いずれのユーザも購入可能な状況に置かれ、クライアント 3 a ~ 3 d のユーザがデータ配信サービスに加入するために購入するものである。この配信データ受信装置には、暗号化グループセッション鍵 K_{grx} を復号化するための鍵復号鍵 K_m があらかじめ記憶されている。

【 0 0 4 2 】

図 4 は、配信データ受信装置（またはアダプタ）3 0 0 の構成を示すブロック図である。この配信データ受信装置 3 0 0 は、制御部 3 0、送受信部 3 1、デー

タ復号部 3 2, 鍵復号部 3 3, および鍵復号鍵保持部 3 4 を備えている。

【 0 0 4 3 】

制御部 3 0 は, 送受信部 3 1, データ復号部 3 2, 鍵復号部 3 3, および鍵復号鍵保持部 3 4 を制御するとともに, 後に詳述する加入者の加入および脱退の処理, 脱退に伴うグループセッション鍵 K_{gr} の消去 (または削除, 破壊), 鍵復号鍵 K_m の消去 (または削除, 破壊) 等の処理を行う。

【 0 0 4 4 】

送受信部 3 1 は, インターネット 1 とのインタフェース装置であり, 制御部 3 0 の制御の下, 制御部 3 0 から与えられる受信要求 (後述) をインターネット 1 を介してサーバ 2 に送信する。また, 送受信部 3 1 は, 制御部 3 0 の制御の下, サーバ 2 からインターネット 1 を介して送信されてきた暗号化グループセッション鍵 K_{grx} および暗号化された配信データ (以下「暗号化配信データ」という。) を受信し, それぞれ鍵復号部 3 3 およびデータ復号部 3 2 に与える。

【 0 0 4 5 】

鍵復号鍵保持部 3 4 は, 鍵復号鍵 K_m を保持する。第三者が鍵復号鍵 K_m を容易に読み出すことができないようにするために, 鍵復号鍵 K_m は, ハードウェア回路 (たとえば IC チップ) として鍵復号鍵保持部 3 4 に記憶 (形成) されていることが好ましい。また, 鍵復号鍵 K_m は, 配信データ受信装置ごと (すなわちクライアントごと) に異なるものが記憶されていることが好ましい。

【 0 0 4 6 】

鍵復号部 3 3 は, サーバ 2 から送信された暗号化グループセッション鍵 K_{grx} を鍵復号鍵 K_m によりに復号化し, 復号化により得られたグループセッション鍵 K_{gr} を保持する。なお, データ復号部 3 2 がグループセッション鍵 K_{gr} を保持してもよい。

【 0 0 4 7 】

データ復号部 3 2 は, サーバ 2 から送信された暗号化配信データを, 鍵復号部 3 3 が保持するグループセッション鍵 K_{gr} を用いて復号化し, 復号化により得られた配信データを, 配信データ受信装置 3 0 0 が取り付けられたクライアントに与える。クライアントは, その表示装置 (CRT ディスプレイ, 液晶ディスプレ

イ等)、スピーカ等に、配信データを出力する。これにより、クライアントのユーザは、配信データを視聴、聴視等することができる。なお、配信データは、出力される前にクライアントのハードディスク等の記憶装置(図示略)に記憶されてもよい。

【0048】

後述するように、鍵復号鍵保持部34に記憶された鍵復号鍵 K_m 、および、鍵復号部33が保持するグループセッション鍵 K_{gr} は、クライアントがデータ配信サービスから脱退することによって、制御部30により消去(または削除、破壊)される。

【0049】

図5は、サーバ2およびマルチキャストグループ3に属するクライアント(ここでは、クライアント3cとする。)の処理の流れを示すシーケンス図である。このシーケンス図に示す処理は、サーバ2のデータ配信サービスに未加入のクライアント3cが、データ配信サービスに加入する場合を説明している。

【0050】

まず、クライアント3cは、データ配信サービスに加入していないので、サーバ2が送信した暗号化配信データを受信できるものの、これを復号化できない状態にある。

【0051】

この状態において、クライアント3cのユーザは、まず、配信データ受信装置300を購入し、これをクライアント3cに取り付ける。クライアント3cに取り付けられた配信データ受信装置300には、鍵復号鍵 $K_m(C)$ が記憶されているものとする。

【0052】

配信データ受信装置300をクライアント3cに取り付けることにより、制御部30は、データ配信サービスの加入手続として、受信要求を送受信部31およびインターネット1を介してサーバ2に送信する(ステップS1)。この受信要求には、クライアント3cのクライアント名と、クライアント3cに取り付けられた配信データ受信装置300を他の配信データ受信装置からユニークに識別す

るための機器番号（識別番号，シリアル番号）とが含まれている。

【0053】

この機器番号は，制御部30にあらかじめ記憶されているものが制御部30により送信されてもよいし，配信データ受信装置300の基板等に貼付されているものが，クライアント3cのユーザによってクライアント3cから入力され，制御部30によって送信されてもよい。また，この機器番号は，配信データ受信装置3の購入後，直ちに販売店からサーバ2に通知され，制御部20に記憶される。

【0054】

クライアント3cからインターネット1を介して送信された受信要求は，サーバ2の送受信部23（図2参照）を介して制御部20に与えられる。制御部20は，受信要求に含まれる機器番号が，販売店から通知されたものであるかどうかを確認し，受信を許可するかどうかを判断する（ステップS21）。

【0055】

制御部20は，受信要求に含まれる機器番号が販売店から通知されたものである場合には受信を許可し（ステップS21でYES），そうでない場合には受信を許可しない（ステップS21でNO）。

【0056】

受信を許可しない場合に，制御部20は，受信要求を無視する（ステップS33）。これにより，クライアント3cは，配信データを視聴または聴視することができない状態が続くこととなる。

【0057】

受信を許可する場合に，制御部20は，加入者リストのリストセルを生成し，生成したリストセルを加入者リストデータベース25の加入者リストに追加する（ステップS23）。このリストセルのクライアント名の欄には，受信要求に含まれるクライアント名が格納され，鍵復号鍵の欄には，配信データ受信装置300の鍵復号鍵保持部34に記憶された鍵復号鍵（「Km(C)」とする。）が格納される。また，加入日時として，受信要求の受信日時（またはリストセル生成日時，データベース25への登録日時等）が格納される。

【 0 0 5 8 】

鍵復号鍵 K_m が配信データ受信装置 3 0 0 ごとに異なる場合には、配信データ受信装置 3 0 0 の機器番号と、その鍵復号鍵保持部 3 4 に記憶された鍵復号鍵 K_m とを対応させた機器番号／鍵復号鍵対応データがサーバ 2（たとえば制御部 2 0 または図示しない記憶部）にあらかじめ記憶される。これにより、制御部 2 0 は、機器番号に対応する鍵復号鍵 K_m をリストセルの鍵復号鍵に格納する。

【 0 0 5 9 】

続いて、鍵暗号部 2 2 は、グループセッション鍵 K_{gr} を鍵復号鍵 $K_m(C)$ により暗号化グループセッション鍵 K_{grx} に暗号化し、暗号化グループセッション鍵 K_{grx} を送受信部 2 3 を介してユニキャストによりクライアント 3 c に送信する（ステップ S 2 5）。

【 0 0 6 0 】

配信データ受信装置 3 0 0 の送受信部 3 1 は、暗号化グループセッション鍵 K_{grx} を受信すると、受信した暗号化グループセッション鍵 K_{grx} を鍵復号部 3 3 に与える。鍵復号部 3 3 は、鍵復号鍵保持部 3 4 が保持する鍵復号鍵 $K_m(C)$ により暗号化グループセッション鍵 K_{grx} を復号化し、復号化されたグループセッション鍵 K_{gr} を保持する（ステップ S 5）。これにより、加入手続は完了する。

【 0 0 6 1 】

その後、サーバ 2 のデータ暗号部 2 1 は、コンテンツデータベース 2 4 に記憶された配信データをグループセッション鍵 K_{gr} により暗号化し、送受信部 2 3 を介して IP マルチキャストによりマルチキャストグループ 3 に送信する（ステップ S 2 7）。

【 0 0 6 2 】

クライアント 3 c の送受信部 3 1 は、暗号化配信データを受信すると、この暗号化配信データを、データ復号部 3 2 に与える。データ復号部 3 2 は、鍵復号部 3 3 が保持するグループセッション鍵 K_{gr} により暗号化配信データを復号化し、復号化した配信データをクライアント 3 c に与える。クライアント 3 c は、配信データに映像データが含まれる場合には、該映像データを表示装置に表示し、音声データが含まれる場合には、該音声をスピーカから出力する（ステップ S 7）

【 0 0 6 3 】

このようなステップ S 5 および S 7 の処理が、クライアント 3 c がデータ配信サービスから脱退するまで繰り返される（ステップ S 9 で N O ）。

【 0 0 6 4 】

一方、クライアント 3 c がデータ配信サービスから脱退する場合には（ステップ S 9 で Y E S ），クライアント 3 c から脱退要求が制御部 3 0 に与えられる。この脱退要求は、たとえば、クライアント 3 c のユーザがクライアント 3 c の入力装置（キーボード等）を介して入力したものである。

【 0 0 6 5 】

制御部 3 0 は、クライアント 3 c から脱退要求を受信すると、鍵復号鍵保持部 3 4 に保持された鍵復号鍵 K m (C) を消去（または削除、破壊）するとともに、鍵復号部 3 3 に保持されたグループセッション鍵 K g r を消去（または削除、破壊）する。そして、制御部 3 0 は、この消去に伴い、消去したことを示すデータとして消去値を生成する（ステップ S 1 1 ）。

【 0 0 6 6 】

この消去値としては、たとえば、配信データ受信装置 3 0 0 の機器番号やクライアントの I P アドレス等に所定の演算（所定の方程式による演算、ハッシュ演算等）を施したものを使用することができる。また、配信データがストリームデータであり、ストリーミングごとに番号が付加されている場合には、このインデックス番号に所定の演算を施したものを消去値として使用することもできる。さらに、脱退要求送信時（配信データの受信終了時）の日時に所定の演算を施したものを消去値として使用することもできる。所定の演算は、配信データ受信装置 3 0 0 のハードウェア回路（たとえば I C チップ）により実行され、どのような演算が実行されているかを第三者が容易に知ることができないようになっている。

【 0 0 6 7 】

制御部 3 0 は、生成した消去値をクライアント名とともに、送受信部 3 1 を介してサーバ 2 に送信する（ステップ S 1 1 ）。

【 0 0 6 8 】

配信データ受信装置 3 0 0 において、鍵復号鍵 $K_m(C)$ およびグループセッション鍵 K_{gr} が消去されることにより、その後、クライアント 3 c は、暗号化配信データを受信するが、これを復号化できなくなる。その結果、クライアント 3 c のユーザは配信データを視聴、聴視等できなくなる。

【 0 0 6 9 】

サーバ 2 の制御部 2 0 は、消去値が正しいかどうかを判断する（ステップ S 2 9）。この判断は、制御部 2 0 が制御部 3 0 と同じ演算を行い、その演算結果と受信した消去値とを比較することにより行われる。たとえば、消去値として、機器番号に所定の演算を施したものが使用される場合には、制御部 2 0 も、制御部 3 0 と同じ演算を、消去値を送信した配信データ受信装置 3 0 0（クライアント 3 c）の機器番号に対して実行し、その演算結果と消去値とを比較することにより、消去値が正しいかどうか判断される。

【 0 0 7 0 】

また、インデックス番号に所定の演算を施したものの、または、受信終了日時に所定の演算を施したものが消去値として使用される場合には、消去値に逆演算を施し、逆演算結果が妥当なものかどうかにより、判断が行われる。この場合には、逆演算結果（インデックス番号または受信終了日時）から、クライアント 3 c がストリームデータをどこまで受信したか、または、受信終了日時が判明するので、これらに基づいて従量制課金を行うこともできる。

【 0 0 7 1 】

消去値が正しい場合には（ステップ S 2 9 で YES）、制御部 2 0 は、クライアント 3 c のリストセルの加入日時と消去値を受信した日時とから、サービスに加入していた時間を求め、この時間に基づいて従量制のサービス料金を算出する。このサービス料金は、クライアント 3 c のユーザに課金され、徴収されることとなる。なお、課金および徴収は、加入期間中、一定期間（たとえば 1 箇月）ごとに行い、脱退時は、脱退直前に課金した時点から脱退時までの期間分の課金を行うこともできる。また、消去値からインデックス値または受信終了日時が得られる場合には、このインデックス値または受信終了日時に基づいて従量制の課金

を行うこともできる。

【 0 0 7 2 】

その後、制御部 2 0 は、クライアント 3 c のリストセルを加入者リストデータベース 2 5 の加入者リストから消去する。消去により、その後、クライアント 3 c には、サービスの課金は行われなくなる。

【 0 0 7 3 】

一方、消去値が正しくない場合には（ステップ S 2 9 で NO），制御部 2 0 は、クライアント 3 c を違反者として、クライアント 3 c に警告を送信する（ステップ S 3 5）。

【 0 0 7 4 】

このように、本実施の形態では、IP マルチキャスト通信において、配信データが暗号化されるとともに、データ配信サービスに正規に加入した者のみが復号化鍵を入手する。したがって、IP マルチキャストにおいて、暗号化が適切に行われ、その結果、データ配信サービスに正規に加入した者のみが配信データを視聴、聴視等することができ、それ以外の者に対してはデータの機密性が確保される。また、本実施の形態では、配信データの提供元であるサーバ 2 において、データ配信サービスの加入者を管理／把握することができる。さらに、本実施の形態によると、ペーパービュー方式による課金よりも木目の細かい従量制の課金を行うことができる。

【 0 0 7 5 】

なお、サーバ 2 は、各クライアント（各配信データ受信装置 3 0 0）の鍵復号鍵 K_m を、前述したように機器番号／鍵復号鍵対応データから得るのではなく、配信データ受信装置 3 0 0 が自己の鍵復号鍵 K_m をサーバ 2 の公開鍵 K_p により暗号化してサーバ 2 に送信し、この送信された鍵をサーバ 2 が秘密鍵 K_s を用いて復号化することにより得ることもできる。この場合に、サーバ 2 の機器番号／鍵復号鍵対応データは特に設ける必要はなくなる。この公開鍵および秘密鍵を用いる公開鍵暗号方式としては、RSA（Rivest Shamir Adleman），楕円曲線暗号等を使用することができる。

【 0 0 7 6 】

また、公開鍵基盤（PKI：Public Key Infrastructure）を利用することもできる。すなわち、各クライアントは、データ配信サービスに加入する際に、PKIの認証局からデジタル証明書（公開鍵および秘密鍵のセット）の発行を受ける。そして、サーバ2は、クライアントからの受信要求を受けると、このデジタル証明書の公開鍵（クライアントの公開鍵）を取得し、この公開鍵を用いてグループセッション鍵 K_{gr} を暗号化し、受信要求を送信したクライアントは、暗号化により得られた暗号化グループセッション鍵 K_{grx} をデジタル証明書の秘密鍵により復号化して、グループセッション鍵 K_{gr} を取得することができる。

【0077】

2. 第2の実施の形態

グループセッション鍵 K_{gr} を定期的に更新することにより、配信データの機密性を確保することもできる。

【0078】

図6は、本発明の第2の実施の形態によるマルチキャスト通信システムの全体構成を示すブロック図である。このマルチキャスト通信システムは、インターネット1に接続されたマルチキャストサーバ4と、複数のクライアント5a～5dを有するマルチキャストグループ5とを備えている。このマルチキャスト通信システムの全体構成は、図1に示す第1の実施の形態のものと同一であるので、このマルチキャスト通信システムの全体構成の説明はここでは省略する。

【0079】

図7は、第2の実施の形態によるサーバ4の構成を示すブロック図である。サーバ4は、制御部40、データ暗号部41、鍵暗号部42、送受信部43、コンテンツデータベース44、加入者リストデータベース45、および鍵データベース46を備えている。

【0080】

制御部40は、データ暗号部41、鍵暗号部42、送受信部43、コンテンツデータベース44、鍵データベース45、および加入者リストデータベース46を制御するとともに、後に詳述する加入者の加入および脱退の処理、加入に伴うグループセッション鍵 K_{gr} の配布、従量制による課金等の処理を行う。また、制

御部 4 0 は、グループセッション鍵 K_{gr} を一定時間 T_1 ごとに更新する。

【 0 0 8 1 】

コンテンツデータベース 4 4 は、第 1 の実施の形態におけるコンテンツデータベース 2 4（図 2 参照）と同様のものである。このコンテンツデータベース 4 4 に記憶された配信データは、制御部 4 0 の制御の下、読み出され、データ暗号部 4 1 に与えられる。

【 0 0 8 2 】

データ暗号部 4 1 は、グループセッション鍵（共通鍵） K_{gr} を制御部 4 0 から受け取り、制御部 4 0 の制御の下、コンテンツデータベース 4 4 からの配信データをグループセッション鍵 K_{gr} により暗号化して送受信部 4 3 に与える。暗号化の方法としては、DES 等が用いられる。なお、グループセッション鍵 K_{gr} は、データ暗号部 4 1 が保持していてもよい。

【 0 0 8 3 】

加入者リストデータベース 4 6 は、第 1 の実施の形態における加入者リストデータベース 2 5（図 2 参照）と同様に構成され、所定の加入手続を経てデータ配信サービスに加入した加入者のリストを記憶する。この加入者リストは、図 3 に示す第 1 の実施の形態のものとほぼ同じであるが、本実施の形態では、第 1 の実施の形態における鍵復号鍵 K_m の欄は設けられない。

【 0 0 8 4 】

鍵データベース 4 5 は、図 8 に示すように、複数のグループセッション鍵 K_{gr} と、各グループセッション鍵 K_{gr} に対応する鍵更新鍵 K_u とが対応した鍵データを保持する。

【 0 0 8 5 】

符号 i を任意の正の整数とすると、グループセッション鍵 $K_{gr}(i+1)$ は、グループセッション鍵 $K_{gr}(i)$ に、これに対応する鍵更新鍵 $K_u(i)$ を作用させることにより得られる。この作用として、たとえばグループセッション鍵 $K_{gr}(i)$ と鍵更新鍵 $K_u(i)$ とを所定の方程式に代入して演算する処理（グループセッション鍵 $K_{gr}(i)$ を鍵更新鍵 $K_u(i)$ により暗号化する処理を含む。）がある。グループセッション鍵 $K_{gr}(1)$ は、グループセッション鍵の初期値として、鍵デー

データベース45にあらかじめ与えられる。

【0086】

これら複数のグループセッション鍵 K_{gr} 群は、任意のグループセッション鍵 $K_{gr}(i)$ で暗号化されたデータが同一のグループセッション鍵 $K_{gr}(i)$ でのみ復号化でき、他のグループセッション鍵 $K_{gr}(j)$ ($i \neq j$) では復号化できないように構成されている。

【0087】

制御部40は、グループセッション鍵 K_{gr} を一定時間 T_1 ごとに $K_{gr}(i)$ から $K_{gr}(i+1)$ に更新して行く。そして、制御部40は、この更新時（更新タイミング）に、鍵更新鍵 $K_u(i)$ をグループセッション鍵 $K_{gr}(i)$ により暗号化し、暗号化した鍵更新鍵をマルチキャストグループ5に属するクライアントに送信する。

【0088】

なお、鍵更新鍵 $K_u(i)$ は、次々と新しいものが制御部40により生成されてもよいし、所定の個数 n だけがあらかじめ用意されていてもよい。前者の場合には、たとえば擬似乱数発生器により発生された擬似乱数等を、新たな鍵更新鍵として使用することができる。後者の場合には、第 n 番目のグループセッション鍵 $K_{gr}(n)$ に鍵更新鍵 $K_u(n)$ を作用させると、第1番目のグループセッション鍵 $K_{gr}(1)$ が生成されるようなサイクリックな構成とされる。

【0089】

また、鍵データベース45には、必ずしも複数のグループセッション鍵が記憶されている必要はなく、現在有効なグループセッション鍵 K_{gr} （すなわち現在、配信データの暗号化に使用されているグループセッション鍵 K_{gr} ）のみが記憶されていてもよい。この場合に、制御部40は、鍵更新時に、現在有効なグループセッション鍵 $K_{gr}(i)$ に、これに対応する鍵更新鍵 $K_u(i)$ を作用させることにより、次のグループセッション鍵 $K_{gr}(i+1)$ を作成して行くこととなる。

【0090】

鍵暗号部42は、制御部40からグループセッション鍵 $K_{gr}(i)$ を受け取る。そして、鍵暗号部42は、制御部40のグループセッション鍵の更新時に、グル

ープセッション鍵 $K_{gr}(i)$ に対応する鍵更新鍵 $K_u(i)$ を鍵データベース 4 5 から読み出してグループセッション鍵 $K_{gr}(i)$ により暗号化し、暗号化された鍵更新鍵 $K_u(i)$ (以下「暗号化鍵更新鍵 $K_{ux}(i)$ 」という。) を送受信部 4 3 に与える。この暗号化鍵更新鍵 $K_{ux}(i)$ は、送受信部 4 3 からインターネット 1 を介してマルチキャストグループ 5 に属するクライアントに送信される。暗号化の方法としては、DES 等が用いられる。

【0091】

送受信部 4 3 は、インターネット 1 とのインタフェース装置であり、制御部 2 0 の制御の下、データ暗号部 4 1 または鍵暗号部 4 2 からのデータをインターネット 1 を介してマルチキャストグループ 5 に属するクライアントに送信するとともに、マルチキャストグループ 5 に属するクライアントからインターネット 1 を介して送信されてきたデータを受信し、制御部 4 0 に与える。

【0092】

図 9 は、第 2 の実施の形態によるクライアント 5 a ~ 5 d のそれぞれの構成を示すブロック図である。クライアント 5 a ~ 5 d はいずれも同じ構成を有するので、以下では、クライアント 5 c を代表として説明することとする。

【0093】

クライアント 5 c は、制御部 5 0、送受信部 5 1、データ復号部 5 2、鍵復号部 5 3、出力部 5 4、入力部 5 5、および鍵生成部 5 6 を備えている。

【0094】

制御部 5 0 は、送受信部 5 1、データ復号部 5 2、鍵復号部 5 3、出力部 5 4、および入力部 5 5 を制御するとともに、後に詳述する加入者の加入および脱退の処理、脱退に伴うグループセッション鍵 $K_{gr}(i)$ の消去（削除、破壊）等の処理を行う。

【0095】

送受信部 5 1 は、インターネット 1 とのインタフェース装置であり、制御部 5 0 の制御の下、制御部 5 0 から与えられる受信要求（後述）をインターネット 1 を介してサーバ 4 に送信する。また、送受信部 5 1 は、制御部 5 0 の制御の下、サーバ 4 からインターネット 1 を介して送信されてきた暗号化配信データおよび

暗号化鍵更新鍵 $K_{ux}(i)$ を受信し、それぞれデータ復号部 52 および鍵復号部 53 に与える。

【0096】

鍵復号部 53 は、サーバ 4 から送信される暗号化鍵更新鍵 $K_{ux}(i)$ をグループセッション鍵 $K_{gr}(i)$ で復号化し、復号化により得られた鍵更新鍵 $K_u(i)$ を保持する。なお、復号化により得られた鍵更新鍵 $K_u(i)$ は、鍵生成部 56 に与えられ、保持されてもよい。

【0097】

鍵生成部 56 は、鍵復号部 53 が保持する鍵更新鍵 $K_u(i)$ を受け取り、この鍵更新鍵 $K_u(i)$ と、これに対応するグループセッション鍵 $K_{gr}(i)$ とから、次のグループセッション鍵 $K_{gr}(i+1)$ を生成する。そして、鍵生成部 56 は、現在有効なグループセッション鍵 $K_{gr}(i)$ および次に有効となるグループセッション鍵 $K_{gr}(i+1)$ を保持する。

【0098】

データ復号部 52 は、サーバ 4 から送信される暗号化配信データを、鍵生成部 56 が保持する現在有効なグループセッション鍵 $K_{gr}(i)$ を用いて復号化し、復号化した配信データを出力部 54 に与える。

【0099】

出力部 54 は、表示装置（CRTディスプレイ、液晶ディスプレイ等）および／またはスピーカ等により構成され、データ復号部 52 から与えられた配信データを出力する。これにより、クライアント 5c のユーザは、配信データを視聴、聴視等することができる。なお、配信データは、出力部 54 により出力される前にクライアント 5c のハードディスク等の記憶装置（図示略）に記憶されてもよい。

【0100】

後述するように、鍵生成部 56 に記憶されたグループセッション鍵 $K_{gr}(i)$ および $K_{gr}(i+1)$ は、クライアント 5c がデータ配信サービスから脱退することによって、制御部 50 により消去（または削除、破壊）される。

【0101】

図 1 0 は、サーバ 4 およびマルチキャストグループ 5 に属するクライアント（ここでは、クライアント 5 c とする。）の処理の流れを示すシーケンス図である。このシーケンス図に示す処理は、サーバ 4 のデータ配信サービスに未加入のクライアント 5 c が、データ配信サービスに加入する場合を説明している。

【 0 1 0 2 】

まず、クライアント 5 c の制御部 5 0 は、クライアント 5 c の入力部 5 5 を介して与えられるユーザの指示に従って、データ配信サービスの加入手続を行う。この加入手続は、制御部 5 0 が受信要求を送受信部 5 1 およびインターネット 1 を介してサーバ 4 に送信することにより行われる（ステップ S 5 1）。この受信要求には、クライアント 5 c のクライアント名が含まれる。

【 0 1 0 3 】

受信要求は、サーバ 4 の送受信部 4 3 を介して制御部 4 0 に与えられる。制御部 4 0 は、受信要求に含まれるクライアント名が、マルチキャストグループ 5 に属するクライアントのもので、かつ、データ配信サービスに加入していないものであるかどうかを確認し、受信を許可するかどうかを判断する（ステップ S 8 1）。

【 0 1 0 4 】

制御部 4 0 は、受信要求に含まれるクライアント名がマルチキャストグループ 5 に属するクライアントのもので、かつ、データ配信サービスに加入していないものである場合には受信を許可し（ステップ S 8 1 で Y E S）、そうでない場合には受信を許可しない（ステップ S 8 1 で N O）。

【 0 1 0 5 】

受信を許可しない場合に、制御部 4 0 は、受信要求を無視する（ステップ S 8 5）。これにより、クライアント 5 c は、配信データを視聴または聴視することができない状態が続くこととなる。

【 0 1 0 6 】

受信を許可する場合に、制御部 4 0 は、クライアント 5 c のための加入者リストのリストセルを生成し、生成したリストセルを加入者リストデータベース 4 6 の加入者リストに追加する（ステップ S 8 3）。このリストセルのクライアント

名の欄には、受信要求に含まれるクライアント名が格納され、加入日時の欄には、受信要求の受信日時（またはリストセル生成日時、データベース 4 6 への登録日時等）が格納される。

【 0 1 0 7 】

続いて、制御部 4 0（または鍵暗号部 4 2）は、受信要求の受信時において有効なグループセッション鍵（ $K_{gr}(i)$ とする。）を暗号化し、送受信部 4 3 を介してクライアント 5 c にユニキャストにより送信する（ステップ S 8 7）。この暗号化の方法としては、たとえば、サーバ 4 が共通鍵 K_c でグループセッション鍵 $K_{gr}(i)$ を暗号化するとともに、この共通鍵 K_c をクライアント 5 c の公開鍵 K_p により暗号化してクライアント 5 c に送信する方法がある。クライアント 5 c は秘密鍵 K_s により、暗号化された共通鍵 K_c を復号化し、さらに暗号化グループセッション鍵 $K_{grx}(i)$ を共通鍵 K_c により復号し、グループセッション鍵 $K_{gr}(i)$ を得る（ステップ S 5 3）。

【 0 1 0 8 】

続いて、鍵暗号部 4 2 は、グループセッション鍵 $K_{gr}(i)$ により鍵更新鍵 $K_u(i)$ を暗号化して暗号化鍵更新鍵 $K_{ux}(i)$ を生成し、この暗号化鍵更新鍵 $K_{ux}(i)$ をクライアント 5 c にユニキャストにより送信する（ステップ S 8 9）。

【 0 1 0 9 】

続いて、データ暗号部 4 1 は、コンテンツデータベース 4 4 に記憶された配信データをグループセッション鍵 $K_{gr}(i)$ により暗号化し、暗号化配信データをマルチキャストグループ 5 にマルチキャスト送信する（ステップ S 9 1）。なお、暗号化鍵更新鍵 $K_{ux}(i)$ のユニキャストによる送信時（ステップ S 8 9）が他のクライアント（群）の鍵更新時（更新タイミング）に該当する場合には、この暗号化鍵更新鍵 $K_{ux}(i)$ は、ユニキャストによりクライアント 5 c にのみ送信されるのではなく、マルチキャストグループ 5 にマルチキャストにより送信されてもよい。

【 0 1 1 0 】

クライアント 5 c の鍵復号部 5 3 は、暗号化鍵更新鍵 $K_{ux}(i)$ をグループセッション鍵 $K_{gr}(i)$ により復号化し、復号化された鍵更新鍵 $K_u(i)$ を保持する

(ステップ S 5 5)。続いて、鍵生成部 5 6 は、グループセッション鍵 $K_{gr}(i)$ に、鍵復号部 5 3 に保持された鍵復号鍵 $K_u(i)$ を作用させて、次のグループセッション鍵 $K_{gr}(i+1)$ を生成し、保持する (ステップ S 5 7)。

【 0 1 1 1 】

一方、データ復号部 5 2 は、暗号化配信データを、グループセッション鍵 $K_{gr}(i)$ により復号化し、復号化により得られた配信データを出力部 5 4 に与える (ステップ S 5 9)。出力部 5 4 は配信データを出力し、これにより、クライアント 5 c のユーザは配信データを視聴、聴視等することができる (ステップ S 6 1)。

【 0 1 1 2 】

サーバ 4 において時間 T_1 ごとの鍵更新タイミングが到来するまで、配信データは、このグループセッション鍵 $K_{gr}(i)$ により暗号化され、送信される (ステップ S 9 3 で NO, S 9 1)。

【 0 1 1 3 】

鍵更新タイミングが到来すると (ステップ S 9 3 で YES)，制御部 4 0 は、グループセッション鍵 $K_{gr}(i)$ を次のグループセッション鍵 $K_{gr}(i+1)$ に更新する (ステップ S 9 5)。

【 0 1 1 4 】

続いて、鍵暗号部 4 2 は、グループセッション鍵 $K_{gr}(i+1)$ に対応する鍵更新鍵 $K_u(i+1)$ をグループセッション鍵 $K_{gr}(i+1)$ により暗号化し、暗号化により得られた暗号化鍵更新鍵 $K_{ux}(i+1)$ をマルチキャストグループ 5 にマルチキャスト送信する (ステップ S 9 7)。

【 0 1 1 5 】

クライアント 5 c の送受信部 5 1 がこの暗号化鍵更新鍵 $K_{ux}(i+1)$ を受信すると、制御部 5 0 は、鍵生成部 5 6 に、グループセッション鍵 $K_{gr}(i)$ を次のグループセッション鍵 $K_{gr}(i+1)$ に更新するように指示する。以後、データ復号部 5 2 は、グループセッション鍵 $K_{gr}(i+1)$ により暗号化配信データを復号化する。直前に使用されていたグループセッション鍵 $K_{gr}(i)$ および鍵更新鍵 $K_u(i)$ は、制御部 5 0 により消去 (または削除、破壊) される。

【0116】

また、これと同時に、鍵復号部53は、暗号化鍵更新鍵 $K_{ux}(i+1)$ をグループセッション鍵 $K_{gr}(i+1)$ により復号化する。鍵生成部56は、グループセッション鍵 $K_{gr}(i+1)$ に、復号化により得られた鍵更新鍵 $K_u(i+1)$ を作用させ、次のグループセッション鍵 $K_{gr}(i+2)$ を生成し、保持する。

【0117】

マルチキャストグループ5に属し、かつ、データ配信サービスに加入している他のクライアントも同様の処理を行う。

【0118】

このようなグループセッション鍵の更新が時間 T_1 ごとに繰り返される。これにより、データ配信サービスに加入していない第三者が、配信データを復号化して視聴、聴視等することが困難となり、配信データの高い機密性が確保される。

【0119】

一方、クライアント5cがデータ配信サービスから脱退する場合には、前述した第1の実施の形態と同様に、制御部50は、鍵生成部56に記憶された現在有効なグループセッション鍵および次のグループセッション鍵、ならびに鍵更新鍵をすべて消去（削除，破壊）する（図10に図示せず）。これにより、クライアント5cは、以後、暗号化配信データを復号化することができず、また、以後のグループセッション鍵の更新も行うことができない。その結果、脱退後、クライアント5cのユーザは、配信データを視聴、聴視等できなくなる。

【0120】

そして、制御部50は、サーバ4に消去値およびクライアント名を送信する（図10に図示せず）。消去値としては、クライアント5cの識別情報（たとえばIPアドレス等）に所定の演算（所定の方程式による演算，ハッシュ演算等）を施したものを使用することができるし、第1の実施の形態と同様にインデックス番号に所定の演算を施したもの、脱退要求送信の日時に所定の演算を施したものを使用することもできる。

【0121】

サーバ4は、消去値が正当かどうかを判断し、正当な場合には、加入者リスト

データベース 4 6 の加入者リストから、消去値を送信したクライアント 5 c のリストセルを消去（削除）する（図 1 0 に図示せず）。消去値が正当でない場合には、サーバ 4 は、消去値を送信したクライアント 5 c に警告等を発する（図 1 0 に図示せず）。これにより、サーバ 4 は、データ配信サービスに加入している加入者を正確に把握することができるとともに、データ配信サービスの課金も適切に行うことができる。課金の方法は、前述した第 1 の実施の形態と同様にして行うことができる。

【 0 1 2 2 】

なお、図 1 0 に示すステップ S 8 7 および S 8 9 に示す送信とともにユニキャストにより行う場合には、暗号化グループセッション鍵 K_{grx} および暗号化鍵更新鍵 K_{ux} を 1 回の送信により、同時に送信することもできる。また、ステップ S 5 3 および／またはステップ S 5 5 において、クライアント 3 c が受信に成功しない場合には、サーバ 4 に再送要求を出し、サーバ 4 に再度送信させることもできる。

【 0 1 2 3 】

また、一定の時間間隔 T_2 ($\neq T_1$) で、データ配信サービスに加入しているクライアントとサーバ 4 とがユニキャスト通信を行い、その時有効なグループセッション鍵を、このグループセッション鍵とは相関関係のない他のグループセッション鍵に変更することもできる。これにより、データ配信サービスに加入していないクライアントが暗号化鍵 K_{gr} を不正に入手した場合であっても、このクライアントがデータ配信サービスに関するデータを復号化することを防止できる。

【 0 1 2 4 】

3. 他の実施の形態

第 1 および第 2 の実施の形態におけるインターネット 1 はイントラネットであってもよい。

【 0 1 2 5 】

また、第 1 のおよび第 2 の実施の形態において、コンテンツデータベース 2 4 (4 4) と加入者リストデータベース 2 5 (4 6) とは、同一のサーバではなく、別々のサーバにそれぞれ保持され、管理されていてもよい。この場合に、マル

チキャストグループ3 (5) に属するクライアントは、加入者リストデータベース25 (46) を保持するサーバ (加入者管理サーバ) に、データ配信サービスへの加入の登録を行い、コンテンツデータベース24 (44) を保持するサーバ (データサーバ) からデータ配信サービスに関するデータを受信することとなる。サービスに加入したクライアントは、グループセッション鍵、鍵更新鍵等を、加入者管理サーバから受け取るようにすることもできるし、データサーバから受け取るようにすることもできる。同様にして、サービス料の課金は、加入者管理サーバが行ってもよいし、データサーバが行ってもよい。

【0126】

第1の実施の形態におけるサーバ2および配信データ受信装置300の各処理は、ハードウェア回路によっても実現できるし、プログラムおよび該プログラムを実行するCPUまたはマイクロコンピュータによっても実現できる。ただし、前述したように、配信データ受信装置300の鍵復号鍵 K_m は、ハードウェア回路またはICチップに形成されていることが好ましい。

【0127】

同様にして、第2の実施の形態におけるサーバ4およびクライアント5の各処理は、ハードウェア回路によっても実現できるし、プログラムおよび該プログラムを実行するCPUまたはマイクロコンピュータによっても実現できる。

【0128】

(付記1) 所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと、マルチキャストグループに属し、前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって、

前記マルチキャストサーバは、

前記データを第1の暗号化鍵により暗号化するデータ暗号部と、

前記データ暗号部により暗号化されたデータを、前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と、

前記第1の暗号化鍵を第2の暗号化鍵により暗号化する鍵暗号部と、

前記鍵暗号部により暗号化された第1の暗号化鍵を、前記マルチキャストグル

ープに属するクライアントのうち、前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と、

を備え、

前記クライアントのうち、前記データ配信サービスに加入したクライアントは

前記鍵送信部により送信される、暗号化された第 1 の暗号化鍵を受信する鍵受信部と、

前記鍵受信部により受信された、暗号化された第 1 の暗号化鍵を復号化鍵により復号化する鍵復号部と、

前記データ送信部により送信される、暗号化されたデータを、前記鍵復号部により得られた第 1 の暗号化鍵により復号するデータ復号部と、

を備えているマルチキャスト通信システム。

【 0 1 2 9 】

(付記 2) 付記 1 において、

前記マルチキャストサーバは、前記マルチキャストグループに属するクライアントのうち、前記データ配信サービスへの加入を希望するクライアントを登録する登録部をさらに備えているマルチキャスト通信システム。

【 0 1 3 0 】

(付記 3) 付記 1 または 2 において、

前記マルチキャストサーバが、前記データ配信サービスに加入したクライアントに対して、時間、または、受信したデータ量に応じた従量制の課金を行う課金部をさらに備えているマルチキャスト通信システム。

【 0 1 3 1 】

(付記 4) 付記 2 において、

前記マルチキャストサーバは、

前記登録部に登録されたクライアントから送信され、該クライアントが自己の保持する少なくとも前記第 1 の暗号化鍵を消去したことを示す消去データを受信する消去データ受信部と、

前記消去データ受信部により消去データが受信されると、該消去データを送信

したクライアントを前記登録部から抹消する抹消部と、

をさらに備え、

前記クライアントは、

前記データ配信サービスから脱退する場合には、自己が保持する少なくとも前記第1の暗号化鍵を消去する消去部と、

前記消去データを生成し、前記消去データを前記マルチキャストサーバに送信する消去データ送信部と、

をさらに備えているマルチキャスト通信システム。

【0132】

(付記5) 付記1から4のいずれか1つにおいて、

前記第2の暗号化鍵と前記復号化鍵とが同一の鍵であるマルチキャスト通信システム。

【0133】

(付記6) 付記5において、

前記第2の暗号化鍵および前記復号化鍵の双方は、前記データ配信サービスに加入したクライアントのそれぞれに個別に設けられた鍵である、マルチキャスト通信システム。

【0134】

(付記7) 付記5または6において、

前記復号化鍵がハードウェア回路または半導体チップにより構成されている、マルチキャスト通信システム。

【0135】

(付記8) 付記1から4のいずれか1つにおいて、

前記第2の暗号化鍵は、前記クライアントが前記第1の復号鍵を前記マルチキャストサーバの公開鍵により暗号化して該マルチキャストサーバに送信し、該マルチキャストサーバが自己の秘密鍵で復号化して得られる鍵である、

マルチキャスト通信システム。

【0136】

(付記9) 付記1から4のいずれか1つにおいて、

前記第 2 の暗号化鍵は、前記データ配信サービスに加入したクライアントに対して公開鍵基盤により発行されたデジタル証明書の公開鍵であり、

前記復号化鍵は、該デジタル証明書の秘密鍵である、

マルチキャスト通信システム。

【 0 1 3 7 】

(付記 1 0) 所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと、マルチキャストグループに属し、前記データを受信する複数のクライアントのうち、前記データ配信サービスに加入したクライアントとの間で行われるマルチキャスト通信方法であって、

前記マルチキャストサーバは、前記データの暗号化に用いられる第 1 の暗号化鍵を第 2 の暗号化鍵により暗号化して、前記マルチキャストグループに属するクライアントのうち、前記データ配信サービスに加入したクライアントにユニキャストにより送信し、

前記クライアントは、前記ユニキャストにより送信される、暗号化された第 1 の暗号化鍵を受信すると、これを復号化鍵により復号化し、

前記マルチキャストサーバは、前記データを前記第 1 の暗号化鍵により暗号化して、前記マルチキャストグループに属するクライアントにマルチキャストにより送信し、

前記クライアントは、前記暗号化されたデータを受信すると、これを前記復号化鍵の復号化により得られた前記第 1 の暗号化鍵により復号化する、

マルチキャスト通信方法。

【 0 1 3 8 】

(付記 1 1) 所定のデータ配信サービスに関するデータを第 1 の暗号化鍵により暗号化するデータ暗号部と、

前記データ暗号部により暗号化されたデータをマルチキャストにより、所定のマルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と、

前記第 1 の暗号化鍵を第 2 の暗号化鍵により暗号化する鍵暗号部と、

前記鍵暗号部により暗号化された第 1 の暗号化鍵を、前記マルチキャストに属

するクライアントのうち、前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と、

を備えているマルチキャストデータ送信装置。

【 0 1 3 9 】

(付記 1 2) 所定のデータ配信サービスに関するデータをマルチキャストにより、所定のマルチキャストグループに属するクライアントに送信するマルチキャストデータ送信方法であって、

前記データの暗号化に用いられる第 1 の暗号化鍵を第 2 の暗号化鍵により暗号化して、前記マルチキャストグループに属するクライアントのうち、前記データ配信サービスに加入したクライアントにユニキャストにより送信し、

前記データを前記第 1 の暗号化鍵により暗号化して、マルチキャストにより前記マルチキャストグループに属するクライアントに送信する、

マルチキャストデータ送信方法。

【 0 1 4 0 】

(付記 1 3) マルチキャストにより送信される、所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信装置であって、

前記データ配信サービスに加入することにより得られる暗号化された第 1 の暗号化鍵を復号化する鍵復号部と、

前記データ配信サービスに関するデータが前記第 1 の暗号化鍵により暗号化されたものを受信するデータ受信部と、

前記データ受信部により受信された、暗号化されたデータを、前記鍵復号部の復号化により得られた第 1 の暗号化鍵により復号化するデータ復号部と、

を備えているマルチキャストデータ受信装置。

【 0 1 4 1 】

(付記 1 4) マルチキャストにより送信される、所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信方法であって、

前記データ配信サービスに加入することにより得られる暗号化された第 1 の暗号化鍵を復号化し、

前記データ配信サービスに関するデータが前記第 1 の暗号化鍵により暗号化さ

れたものを受信し、

前記受信した、暗号化されたデータを、前記復号化により得られた第 1 の暗号化鍵により復号化する、

マルチキャストデータ受信方法。

【 0 1 4 2 】

(付記 1 5) 所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと、マルチキャストグループに属し、前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって、

前記マルチキャストサーバは、

前記データを暗号化するためのデータ暗号化鍵を、所定の更新タイミングごとに、該更新タイミング前に有効なデータ暗号化鍵に、該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある、更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と、

前記更新鍵を生成し、または、あらかじめ保持する更新鍵保持部と、

前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と、

前記データ暗号部により暗号化されたデータを、前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と、

前記更新タイミングごとに、更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を、該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と、

前記更新タイミングごとに、前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と、

を備え、

前記複数のクライアントのうち、前記データ配信サービスに加入したクライアントは、

前記データ送信部により送信される、暗号化されたデータを受信するデータ受信部と、

前記データ受信部により受信される、前記暗号化されたデータを、前記現在有効なデータ暗号化鍵と同一の現在有効なデータ復号化鍵により復号化するデータ復号部と、

前記更新鍵送信部により送信される、暗号化された更新鍵を受信する更新鍵受信部と、

前記更新鍵受信部により受信される、暗号化された更新鍵を、前記現在有効なデータ復号化鍵により復号化する更新鍵復号部と、

前記データ配信サービスへの加入時には、外部から与えられ、その後は、前記更新タイミングごとに、該更新タイミング前に有効なデータ復号化鍵に、該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより、更新タイミング後に有効なデータ復号化鍵を生成し、前記更新タイミングごとに、前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新するデータ復号化鍵更新部と、
を備えているマルチキャスト通信システム。

【 0 1 4 3 】

(付記 1 6) 所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと、マルチキャストグループに属し、前記データを受信する複数のクライアントうち、前記所定のデータ配信サービスに加入したクライアントとを間で行われるマルチキャスト通信方法であって、

前記マルチキャストサーバは、前記データを現在有効なデータ暗号化鍵により暗号化して、前記マルチキャストグループに属するクライアントにマルチキャストにより送信し、

前記クライアントは、前記マルチキャストサーバから送信される、暗号化されたデータを受信して、前記暗号化されたデータを前記現在有効なデータ暗号化鍵と同一の現在有効なデータ復号化鍵により復号化し、

前記マルチキャストサーバは、前記データ暗号化鍵を、所定の更新タイミングごとに、該更新タイミング前に有効なデータ暗号化鍵に、該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある、更新タイミング後に有効となるデータ暗号化鍵に更新し、

前記マルチキャストサーバは、前記更新タイミングごとに、更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を、該更新タイミング後に有効なデータ暗号化鍵により暗号化して、前記クライアントにユニキャストまたはマルチキャストにより送信し、

前記クライアントは、前記マルチキャストサーバから送信される、暗号化された更新鍵を受信して、該暗号化された更新鍵を、前記現在有効なデータ復号化鍵により復号化し、

前記クライアントは、前記データ配信サービスへの加入時には、外部から与えられ、その後は、前記更新タイミングごとに、該更新タイミング前に有効なデータ復号化鍵に、該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより、更新タイミング後に有効なデータ復号化鍵を生成し、前記更新タイミングごとに、前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新する、
マルチキャスト通信方法。

【 0 1 4 4 】

(付記 1 7) 所定のデータ配信サービスに関するデータを暗号化するためのデータ暗号化鍵を、所定の更新タイミングごとに、該更新タイミング前に有効なデータ暗号化鍵に、該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある、更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と、

前記更新鍵を生成し、または、あらかじめ保持する更新鍵保持部と、

前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と、

前記データ暗号部により暗号化されたデータを、所定のマルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と、

前記更新タイミングごとに、更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を、該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と、

前記更新タイミングごとに、前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と

を備えているマルチキャストデータ送信装置。

【 0 1 4 5 】

(付記 1 8) 所定のデータ配信サービスに関するデータをマルチキャストにより、所定のマルチキャストグループに属するクライアントに送信するマルチキャストデータ送信方法であって、

前記データを現在有効なデータ暗号化鍵により暗号化して、前記マルチキャストグループに属するクライアントにマルチキャストにより送信し、

前記データ暗号化鍵を、所定の更新タイミングごとに、該更新タイミング前に有効なデータ暗号化鍵に、該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある、更新タイミング後に有効となるデータ暗号化鍵に更新し、

前記更新タイミングごとに、更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を、該更新タイミング後に有効なデータ暗号化鍵により暗号化して、前記クライアントにユニキャストまたはマルチキャストにより送信する、

マルチキャストデータ送信方法。

【 0 1 4 6 】

(付記 1 9) マルチキャストサーバからマルチキャストにより送信される、所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信装置であって、

所定の更新タイミングごとに更新されるデータ暗号化鍵のうち、現在有効なデータ暗号化鍵によって、前記データが暗号化されたものを受信するデータ受信部と、

前記データ受信部により受信される、前記暗号化されたデータを、前記現在有効なデータ暗号化鍵と同一の現在有効なデータ復号化鍵により復号化するデータ復号部と、

前記データ復号化鍵を更新するために使用される更新鍵が前記現在有効なデータ暗号化鍵により暗号化されたものを前記マルチキャストサーバから受信する更新鍵受信部と、

前記更新鍵受信部により受信される、暗号化された前記更新鍵を、前記現在有効なデータ復号化鍵により復号化する更新鍵復号部と、

前記データ配信サービスへの加入時には、外部から与えられ、その後は、所定の更新タイミングごとに、該更新タイミング前に有効なデータ復号化鍵に、該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより、更新タイミング後に有効なデータ復号化鍵を生成し、前記更新タイミングごとに、前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新するデータ復号化鍵更新部と

を備えているマルチキャストデータ受信装置。

【0147】

(付記20) マルチキャストサーバからマルチキャストにより送信される、所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信方法であって、

所定の更新タイミングごとに更新されるデータ暗号化鍵のうち、現在有効なデータ暗号化鍵によって、前記データが暗号化されたものを受信し、

前記受信した、前記暗号化されたデータを、前記現在有効なデータ暗号化鍵と同一の現在有効な復号化鍵により復号化し、

前記データ復号化鍵を更新するために使用される更新鍵が前記現在有効なデータ暗号化鍵により暗号化されたものを前記マルチキャストサーバから受信し、

前記暗号化された前記更新鍵を、前記現在有効なデータ復号化鍵により復号化し、

前記データ配信サービスへの加入時には、外部から与えられ、その後は、所定の更新タイミングごとに、該更新タイミング前に有効なデータ復号化鍵に、該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより、更新タイミング後に有効なデータ復号化鍵を生成し、前記更新タイミングごとに、前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新する、

マルチキャストデータ受信方法。

【0148】

【発明の効果】

本発明によると、マルチキャスト通信において、データの暗号化を適切に行うことができる。また、本発明によると、マルチキャストサーバまたはデータ配信サービスの加入者を管理するサーバは、マルチキャストグループに属するクライアントのうち、データ配信サービスに加入しているクライアントを把握できる。さらに、本発明によると、加入から脱退時までのデータ受信量に応じた課金を行ったり、あるいは、加入から脱退までの時間に応じた課金を行うことにより、木目の細かい従量制課金を行うことができる。

【図面の簡単な説明】

【図1】

本発明の第1の実施の形態によるマルチキャスト通信システムの全体構成を示すブロック図である。

【図2】

第1の実施の形態によるマルチキャストサーバの構成を示すブロック図である。

【図3】

加入者リストのデータ構造を示す。

【図4】

配信データ受信装置（またはアダプタ）の構成を示すブロック図である。

【図5】

第1の実施の形態によるサーバおよびマルチキャストグループに属するクライアントの処理の流れを示すシーケンス図である。

【図6】

本発明の第2の実施の形態によるマルチキャスト通信システムの全体構成を示すブロック図である。

【図7】

第2の実施の形態によるマルチキャストサーバの構成を示すブロック図である。

【図 8】

複数のグループセッション鍵と、各グループセッション鍵に対応する鍵更新鍵とが対になった鍵データを示す。

【図 9】

第 2 の実施の形態によるクライアントの構成を示すブロック図である。

【図 1 0】

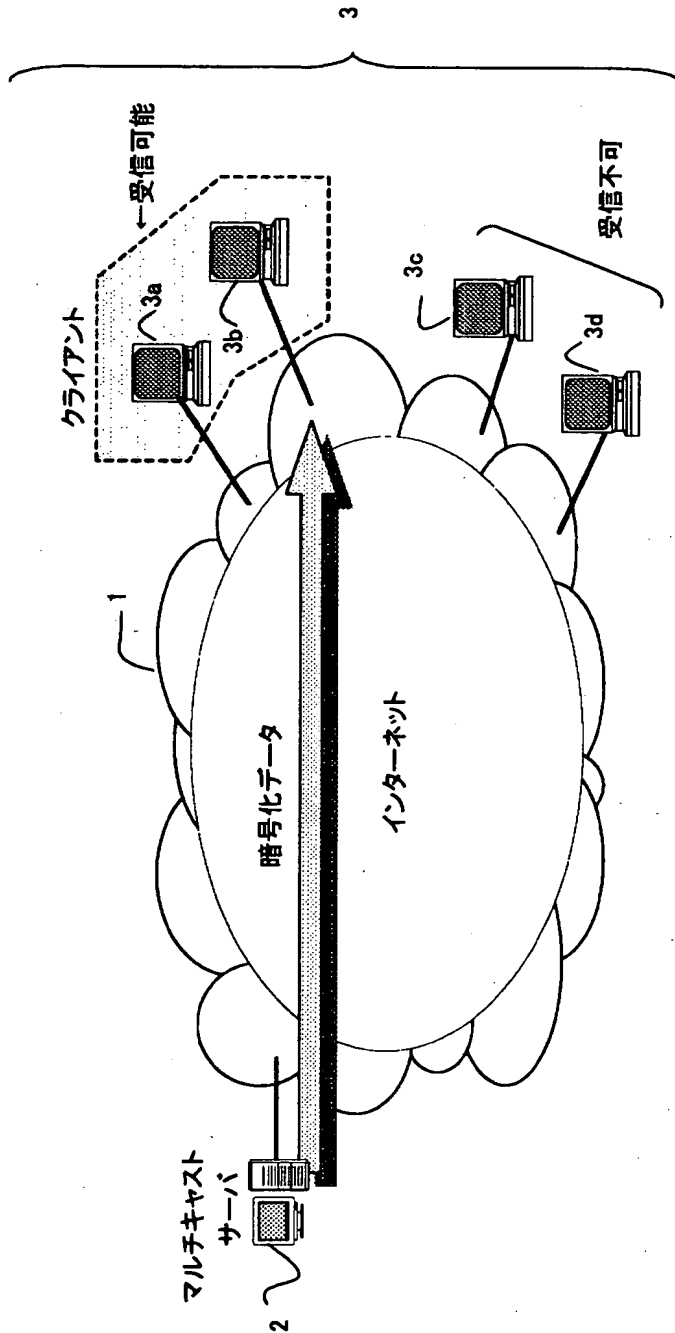
第 2 の実施の形態によるサーバおよびマルチキャストグループに属するクライアントの処理の流れを示すシーケンス図である。

【符号の説明】

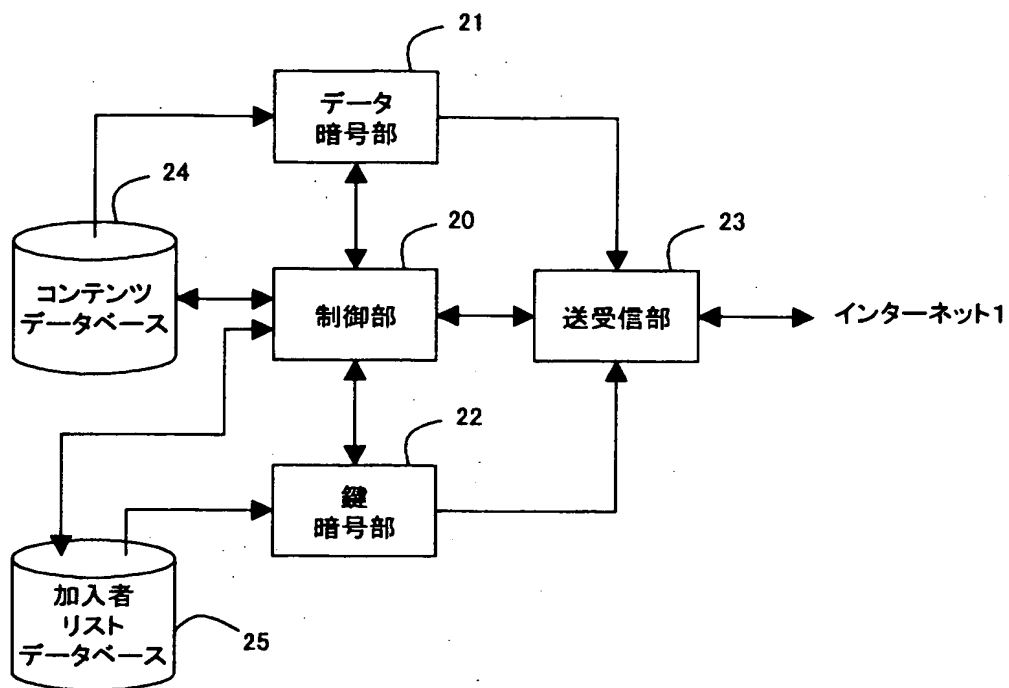
- 1 インターネット
- 2, 4 マルチキャストサーバ
- 3, 5 マルチキャストグループ
- 3 a ~ 3 d, 5 a ~ 5 d クライアント
- 2 0, 3 0, 4 0, 5 0 制御部
- 2 1, 4 1 データ暗号部
- 2 2, 4 2 鍵暗号部
- 2 3, 3 1, 4 3, 5 1 送受信部
- 2 4, 4 4 コンテンツデータベース
- 2 5, 4 6 加入者リストデータベース
- 4 5 鍵データベース
- 3 0 0 配信データ受信装置
- 3 2 データ復号部
- 3 3, 5 3 鍵復号部
- 3 4 鍵復号鍵保持部
- 5 6 鍵生成部

【書類名】 図面

【図 1】



【図 2】

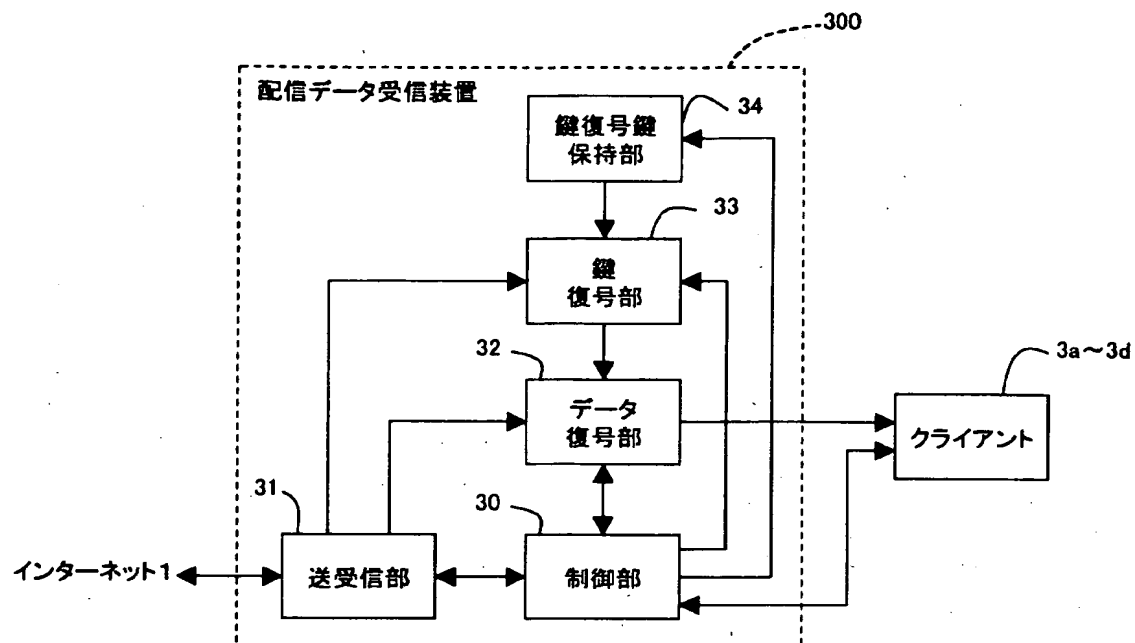


【図 3】

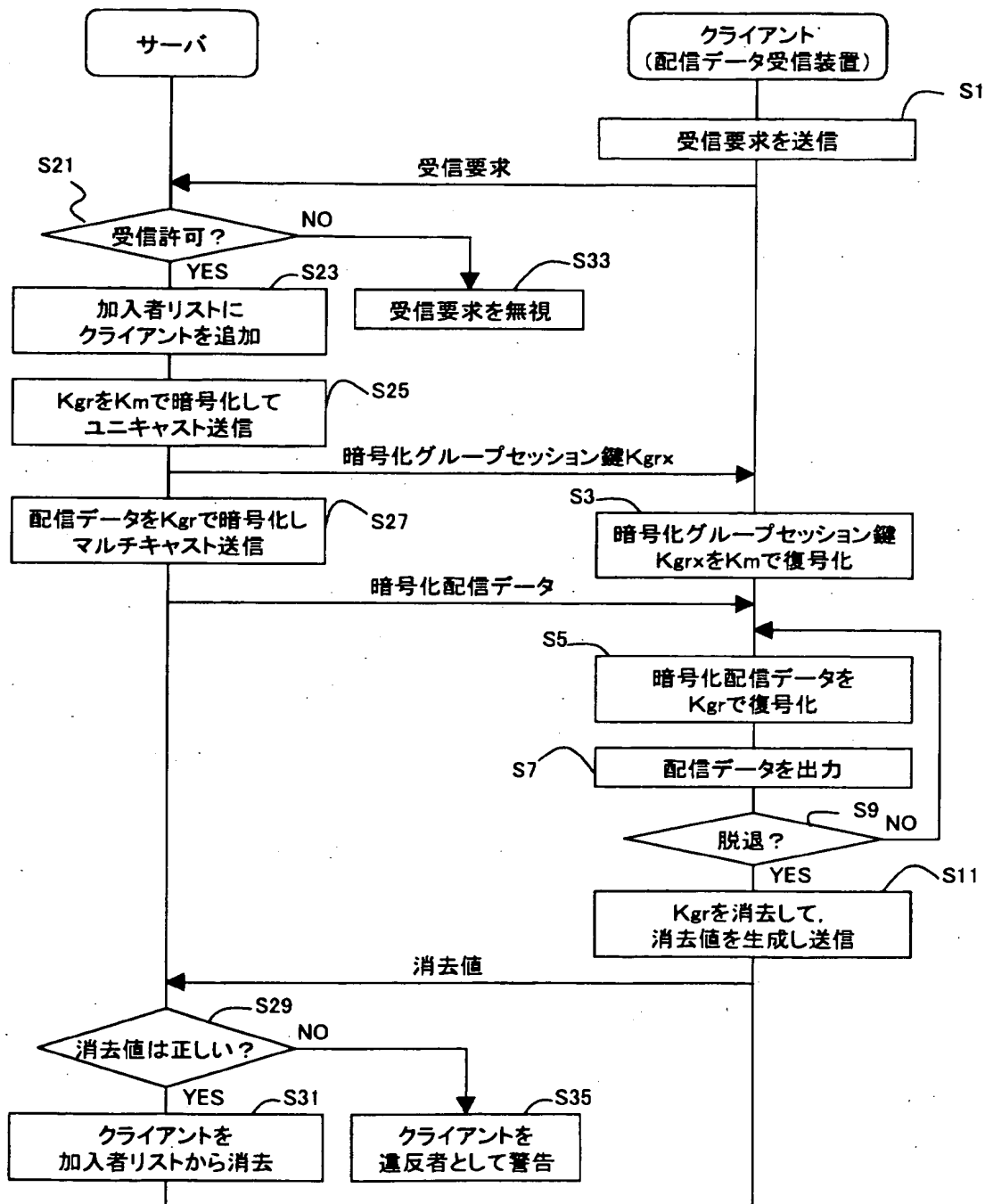
加入者リスト

加入者名	鍵復号鍵	加入日時
クライアントA	$K_m(A)$	$T(A)$
クライアントB	$K_m(B)$	$T(B)$
⋮	⋮	⋮

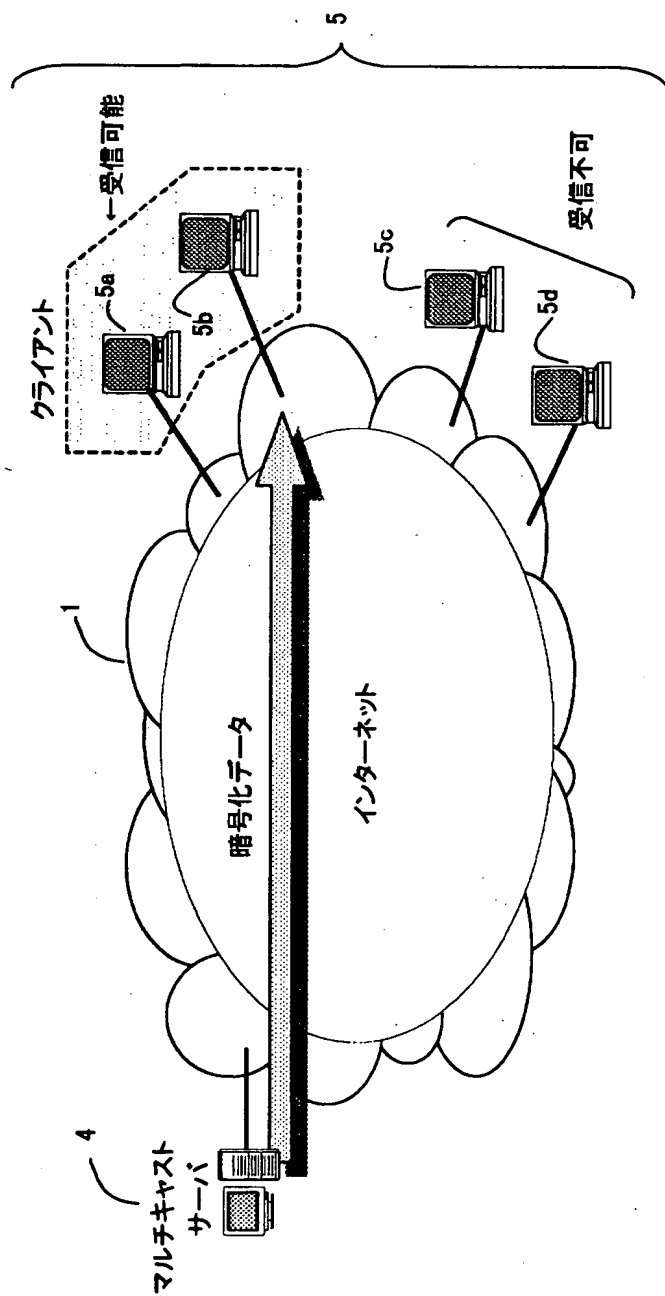
【図 4】



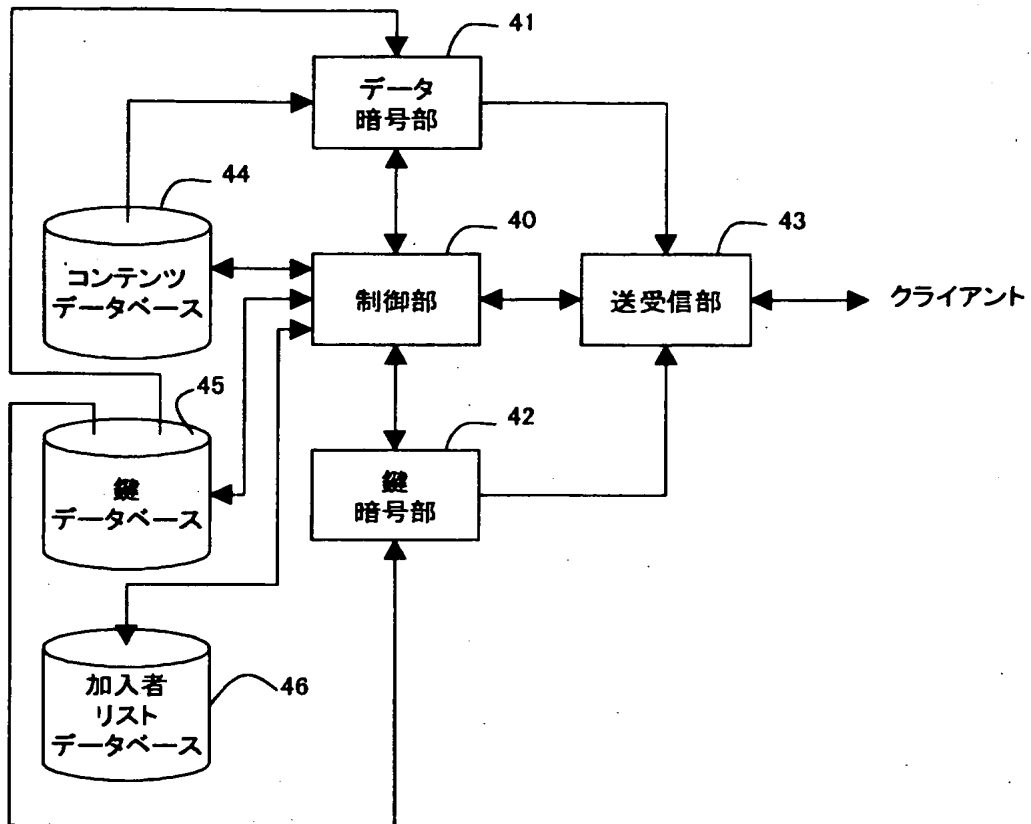
【図 5】



【図 6】



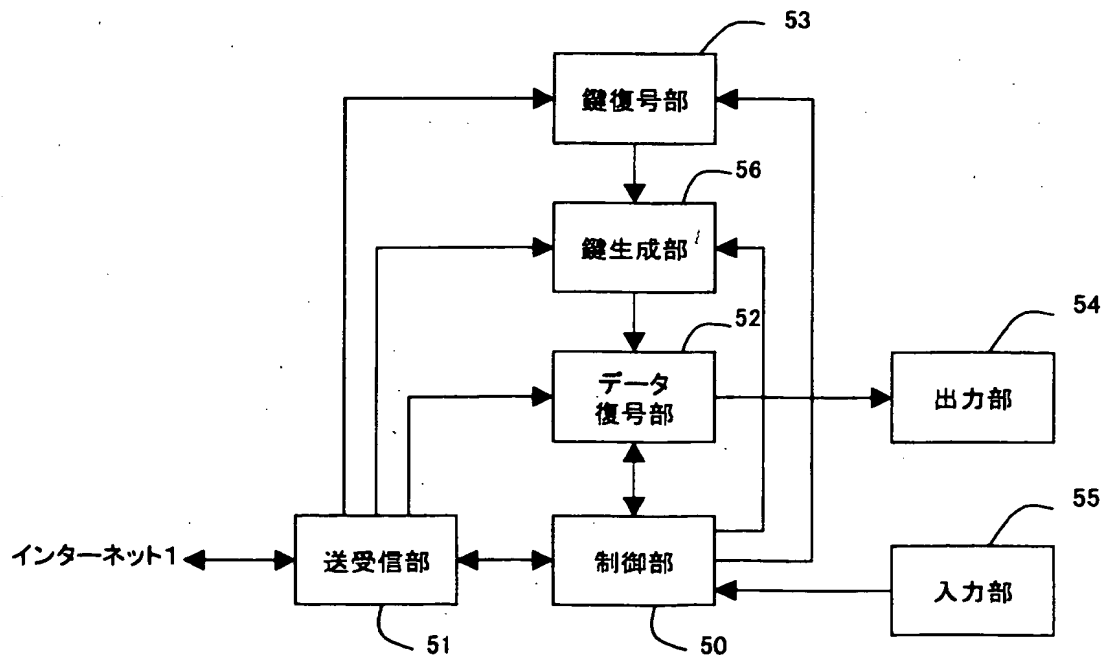
【図 7】



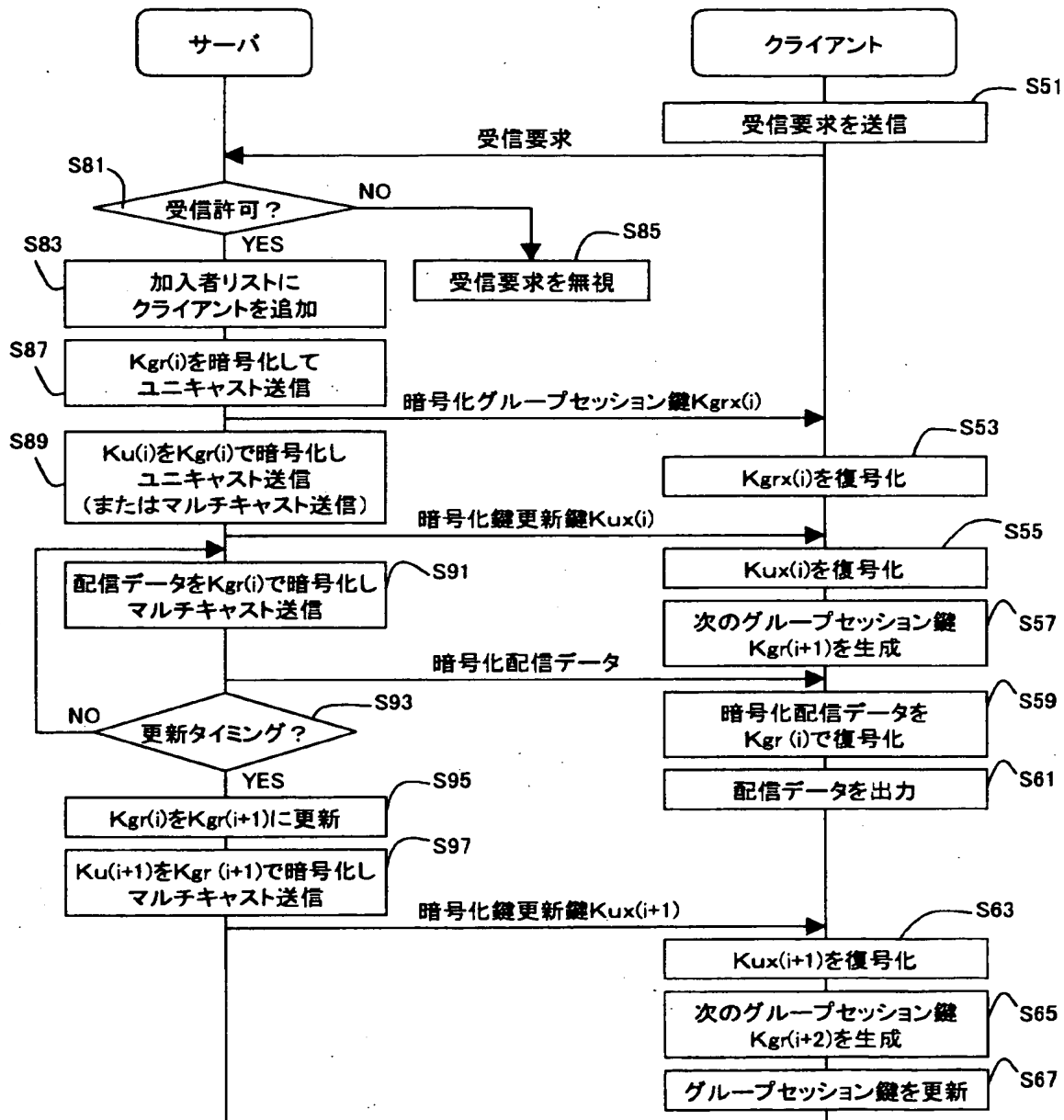
【図 8】

グループ セッション鍵	鍵更新鍵
Kgr (1)	Ku (1)
Kgr (2)	Ku (2)
Kgr (3)	Ku (3)
⋮	⋮
Kgr (i)	Ku (i)
Kgr (i+1)	Ku (i+1)
⋮	⋮

【図 9】



【図10】



【書類名】 要約書

【要約】

【課題】 マルチキャスト通信において暗号化を適切に行う。

【解決手段】 マルチキャストサーバ2は、データ配信サービスに関するデータの暗号化に用いられるグループセッション鍵 K_{gr} を第2の暗号化鍵 K_m により暗号化して、マルチキャストグループ3に属するクライアントのうち、該サービスに加入したクライアントにユニキャストにより送信する。該サービスに加入したクライアントは、ユニキャストにより送信される、暗号化された第1の暗号化鍵を受信すると、これを復号化鍵 K_m により復号化する。続いて、マルチキャストサーバ2は、データを第1の暗号化鍵により暗号化して、マルチキャストグループ3に属するクライアントにマルチキャストにより送信する。クライアントは、暗号化されたデータを受信すると、これを復号化鍵の復号化により得られた第1の暗号化鍵により復号化する。

【選択図】 図5

認定・付加情報

特許出願の番号	特願 2001-258890
受付番号	50101260237
書類名	特許願
担当官	佐藤 一博 1909
作成日	平成 13 年 9 月 4 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
【氏名又は名称】	富士通株式会社
【代理人】	申請人
【識別番号】	100094514
【住所又は居所】	神奈川県横浜市港北区新横浜 3-9-5 第三東 昇ビル 3 階 林・土井 国際特許事務所
【氏名又は名称】	林 恒徳

【代理人】

【識別番号】	100094525
【住所又は居所】	神奈川県横浜市港北区新横浜 3-9-5 第三東 昇ビル 3 階 林・土井 国際特許事務所
【氏名又は名称】	土井 健二

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社